4 行列

4.1 行列の定義と演算

今まですでに、何度も「行列 (Matrix)」という言葉を使ってきましたが、ここで、改めてその定義を述べます。

定義 4.1 1. $m \times n$ 個の数を長方形（矩形）に並べた

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

を (m,n) **行列、又は、** $m \times n$ **行列** と言う。上の行列を略して、$A = [a_{ij}]$ などと書くこともある。

2. 二つの行列は、そのサイズ (m,n) が等しく、かつ、その成分（矩形に並べた $m \times n$ 個の数）が等しいときに等しい。

3. $1 \times n$ 行列 $[a_1, a_2, \ldots, a_n]$ を n **次行ベクトル**、$m \times 1$ 行列、

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}$$

を m **次列ベクトル**という。

4. 上の行列 A において、左から、j 番目の縦に並んだ、

$$\boldsymbol{a}_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

を A の **第** j **列**と言い、上から、i 番目の横に並んだ、

$$\boldsymbol{a}'_i = [a_{i1}, a_{i2}, \ldots, a_{in}]$$

を A の**第** i **行**と言い、A を次のようにも書く。

$$A = [\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n] = \begin{bmatrix} \boldsymbol{a}'_1 \\ \boldsymbol{a}'_2 \\ \vdots \\ \boldsymbol{a}'_m \end{bmatrix}$$

5. 第 i 行 第 j 列を (i,j) **成分**と呼ぶ。上の行列 A は、(i,j) 成分が a_{ij} であるような行列である。

次に行列に演算（足し算とスカラー倍と積）を定義する。

定義 4.2 A、B を共に同じ型（$m \times n$）の行列、c を数（スカラー）とする、**和** $A+B$、**スカラー倍** cA を成分での和と、c 倍とで定義する。すなわち、

$$A+B = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ & \cdots\cdots\cdots & & \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{bmatrix}, cA = \begin{bmatrix} ca_{11} & ca_{12} & \cdots & ca_{1n} \\ ca_{21} & ca_{22} & \cdots & ca_{2n} \\ & \cdots\cdots\cdots & & \\ ca_{m1} & ca_{m2} & \cdots & ca_{mn} \end{bmatrix}$$

ここで、連立一次方程式の解に戻ってみましょう。解を、以下のように書いたのは、上の行列の和とスカラー倍の定義を使って書いたものであることがわかると思います。

$$\begin{cases} x &= -\frac{1}{2}t+\frac{3}{2} \\ y &= -\frac{1}{2}t-\frac{1}{2} \\ z &= t \end{cases} \qquad \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -\frac{1}{2}t+\frac{3}{2} \\ -\frac{1}{2}t-\frac{1}{2} \\ t \end{bmatrix} = t \cdot \begin{bmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 1 \end{bmatrix} + \begin{bmatrix} \frac{3}{2} \\ -\frac{1}{2} \\ 0 \end{bmatrix}$$

定義 4.3 $A=(a_{i,j})$ を (m,r) 行列、$B=(b_{k,l})$ を (r,n) 行列とする。このとき、(m,n) 行列 $C=(c_{s,t})$ の各成分は次のようにして定義されたものとする。

$$c_{s,t} = \sum_{u=1}^{r} a_{s,u}b_{u,t} = a_{s,1}b_{1,t} + a_{s,2}b_{2,t} + \cdots + a_{s,r}b_{r,t}.$$

このとき、$C=AB$ と書き、**行列 A と B の積**という。

$$C = AB = \begin{bmatrix} \sum_{u=1}^{r} a_{1,u}b_{u,1} & \sum_{u=1}^{r} a_{1,u}b_{u,2} & \cdots & \sum_{u=1}^{r} a_{1,u}b_{u,n} \\ \sum_{u=1}^{r} a_{2,u}b_{u,1} & \sum_{u=1}^{r} a_{2,u}b_{u,2} & \cdots & \sum_{u=1}^{r} a_{2,u}b_{u,n} \\ & \cdots\cdots\cdots & & \\ \sum_{u=1}^{r} a_{m,u}b_{u,1} & \sum_{u=1}^{r} a_{m,u}b_{u,2} & \cdots & \sum_{u=1}^{r} a_{m,u}b_{u,n} \end{bmatrix}$$

積は複雑なのでゆっくり見ていきましょう。まず、行列 A と 行列 B をかけるときには、それぞれの行列のサイズが重要です。最初の行列 A の列の数と、後の行列 B の行の数が等しいときだけ積 AB が定義されます。列は縦並びのもので、行は横並びでした。上の定義では、A は (m,r) 行列、B を (r,n) で確かに、A の列の数は r、B の行の数は r で等しいのでかけることができます。サイズは行の数、列の数の順です。「行列」だからまず行の数そして列の数と覚えれば良いでしょう。行という漢字は横の線が多いから行は横、列という漢字は縦の線が多いから列は縦を表すと説明する人もいるようです。到底 universal ではありませんが、確かに覚えるのにはいいかも知れません。さて、かけた結果は、最初の行列の行の数と同じ行の数、後の行列の列の数と同じ数の列をもった行列になります。定義においては、結果は (m,n) 行列になるわけです。さて、成分は、定義では (s,t) 成分が書いてあります。これは、結果の行列の s 行 t 列にある数のことです。結果の行列の s 行 t 列を計算する時には、最初の行列 A の 第 s 行と、後の行列 B の第 t 列を使います。A の 第 s 行は $a_{s,1}, a_{s,2}, \ldots, a_{s,r}$ が横にならんでいます。B の第 t 列

は $b_{1,t}, b_{2,t}, \ldots, b_{r,t}$ が縦にならんでいます。結果は、これらの 1 番目と 1 番目、2 番目と 2 番目、とかけてそれらの和をとったものです。それと、つぎのように表しています。

$$c_{s,t} = \sum_{u=1}^{r} a_{s,u} b_{u,t} = a_{s,1} b_{1,t} + a_{s,2} b_{2,t} + \cdots + a_{s,r} b_{r,t}.$$

うまくこの計算ができるためには、A の第 s 行にある列の数 r と、B の第 t 列にある行の数 r が等しくないといけません。それが実は、最初の積が定義できる条件でした。ここで現れる $\sum_{u=1}^{r} a_{s,u} b_{u,t}$ ですが、最初の $\sum$ はギリシャ語の σ (シグマ) の大文字で英語の s にあたります。和は summation と言いますから、和をとるといういみで Σ が用いられています。その後ろの式、$a_{s,u} b_{u,t}$ のうち u の部分を 1 から順に r まで動かして得られる

$$a_{s,1} b_{1,t}, a_{s,2} b_{2,t}, \ldots, a_{s,r} b_{r,t}$$

の和を表すものです。結果として、右辺に現れる和となります。

なかなか複雑です。例を見てみましょう。次の例では、A は $(2,3)$ 行列、B は $(3,2)$ 行列です。

例 4.1 1. $A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 5 \\ 3 & 6 \\ 4 & 7 \end{bmatrix}$ とすると、

$$\begin{aligned} AB &= \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 3 & 6 \\ 4 & 7 \end{bmatrix} \\ &= \begin{bmatrix} 1\cdot 2 + 0\cdot 3 + 2\cdot 4 & 1\cdot 5 + 0\cdot 6 + 2\cdot 7 \\ 0\cdot 2 + 1\cdot 3 + 1\cdot 4 & 0\cdot 5 + 1\cdot 6 + 1\cdot 7 \end{bmatrix} = \begin{bmatrix} 10 & 19 \\ 7 & 13 \end{bmatrix} \\ BA &= \begin{bmatrix} 2 & 5 \\ 3 & 6 \\ 4 & 7 \end{bmatrix} \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2\cdot 1 + 5\cdot 0 & 2\cdot 0 + 5\cdot 1 & 2\cdot 2 + 5\cdot 1 \\ 3\cdot 1 + 6\cdot 0 & 3\cdot 0 + 6\cdot 1 & 3\cdot 2 + 6\cdot 1 \\ 4\cdot 1 + 7\cdot 0 & 4\cdot 0 + 7\cdot 1 & 4\cdot 2 + 7\cdot 1 \end{bmatrix} = \begin{bmatrix} 2 & 5 & 9 \\ 3 & 6 & 12 \\ 4 & 7 & 15 \end{bmatrix} \end{aligned}$$

このように、AB と、BA は、そのサイズすら違います。また、たとえサイズが等しくても、殆どの場合、$AB \neq BA$ となることに注意して下さい。

2. $A = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 1 & 1 \\ 11 & 1 & 5 \end{bmatrix}$, $\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ とすると、

$$A\boldsymbol{x} = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 1 & 1 \\ 11 & 1 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 3x_1 + x_2 + 2x_3 \\ x_1 + x_2 + x_3 \\ 11x_1 - x_2 + 5x_3 \end{bmatrix}$$

従って、$\boldsymbol{b} = \begin{bmatrix} 4 \\ 1 \\ 17 \end{bmatrix}$ とすると最初に扱った方程式を $A\boldsymbol{x} = \boldsymbol{b}$ と書くことができます。行列が等しいのは、サイズが等しくそれぞれの成分がすべて等しいということでした。ですから、$A\boldsymbol{x} = \boldsymbol{b}$ は連立方程式を表しているわけです。連立一次方程式を $A\boldsymbol{x} = \boldsymbol{b}$ というようなコンパクトな形に書けるようにしたのも、積を、上のように定義した一つの理由です。

3. 一般には、

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},\ \boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},\ \boldsymbol{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

とすると、$A\boldsymbol{x} = \boldsymbol{b}$ と書ける。その意味は、

$$A\boldsymbol{x} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

が成り立つ事と、各成分が等しいこととが同値だからです。

Note.

1. ２つの行列に対して、積がいつも定義できるわけではありませんが、A, B を共に、(n,n) 行列とすると、AB も、BA も共に定義することが出来、どちらも (n,n) 行列となります。この様に、行の数と、列の数が等しい行列はとくに重要です。これを n 次正方行列、又は、単に 正方行列と言います。

2. すべて成分が零の (m,n) 行列を 零行列と言い、$\mathbf{0} = \mathbf{0}_{m,n}$ と書きます。A を $m \times n$ 行列とすると、

$$A + \mathbf{0}_{m,n} = \mathbf{0}_{m,n} + A = A,\ A\mathbf{0}_{n,l} = \mathbf{0}_{m,l},\ \mathbf{0}_{l,m}A = \mathbf{0}_{l,n}$$

が成り立ちます。すべての成分が 0 ですから当たり前ですね。$\mathbf{0}_{n,n}$ を簡単に $\mathbf{0}_n$ と書くこともあります。

3. 正方行列において、i 行 i 列の成分（(i,i) 成分）を対角成分と言います。正方行列を矩形に書くと、行の数と列のかずが同じですが、その左上から右下に伸びる対角線の部分に (i,i) 成分があるからです。n 次正方行列で、対角成分がすべて 1 他は、すべて 0 であるような行列を、単位行列と言い、$I = I_n$ とかきます。（高校の教科書など、教科書によっては、$E = E_n$ を使っているものもあります。しかしかけ算の 1 に対応するものですから、I をここでは使うことにします。）簡単に確かめられるように、A を (m,n) 行列、B を (n,m) 行列とすると、$A \cdot I = A$、$I \cdot B = B$ となっています。

命題 4.1 行列の演算に関して次の諸性質が成り立つ。

(1) $A+B=B+A$ （加法に関する交換法則）

(2) $A+(B+C)=(A+B)+C$ （加法に関する結合法則）

(3) $A(BC)=(AB)C$ （乗法に関する結合法則）

(4) $A(B+C)=AB+AC$、$(A+B)C=AC+BC$ （分配法則）

(5) $cA=(cI)A$

証明もそう難しくはありませんが、ここでは省きます。大切なのは割算を除いて大体の計算が数の場合と似た法則にしたがってできること、しかし積に関しては交換法則 $AB=BA$ が成り立たないことです。もちろん、成り立つ場合もあります。たとえば A を n 次正方行列、$I=I_n$、$O=O_n$ とすれば、

$$A\cdot I=A=I\cdot A,\ A\cdot O=O=O\cdot A.$$

もう一つ、積においては、行列のサイズに常に注意して計算をしないといけないと言うことです。

4.2 行列の積と連立一次方程式

連立一次方程式について考えてきました。もう一度道筋を復習してみましょう。

Step 1. 連立一次方程式の拡大係数行列を作りそれを B とする。

Step 2. B に行に関する基本変形を何回か施して既約ガウス行列 C を得る。

Step 3. C から得られる情報をもとに、基本定理を適用して、解の存在・非存在、一つにきまるかどうか、無限個の場合のパラメーターの数を決定する。

ここで問題がありました。

1. C を拡大係数行列として求めた解は、本当に最初の B を拡大係数行列とする連立一次方程式の解になっているのか。(C の解 $\Rightarrow$ B の解？)
2. B を拡大係数行列とする連立一次方程式の解はすべて最後の C を拡大係数行列として求めた解に含まれているのか。(B の解 $\Rightarrow$ C の解？)

さて、一番簡単な一次方程式を考えてみましょう。たとえば $2\cdot x=4$。これを解くには、両辺を 2 で割ります。連立一次方程式は、A を係数行列とすると、行列の積を用いて $A\boldsymbol{x}=\boldsymbol{b}$ と表すことができることを前の節で見ました。それなら A で割ることによって $\boldsymbol{x}$ を求める方法はないでしょうか。上に掲げた問題とともにこの問題を考えるのが、これからの主題です。

もう一度簡単な一次方程式を考えてみましょう。$ax=b$ これから $x=b/a$ を導くのですが、正確には条件があり、$a\neq 0$ が必要でした。いま考えたいのは、$A\boldsymbol{x}=\boldsymbol{b}$ ですから、$1/A$ のようなものが存在する A の条件も考えないといけなそうです。

さて、$A\boldsymbol{x} = \boldsymbol{b}$ を考えたとき、A に対して $BA = AB = I$ となるような B があったとしましょう。I は大体 1 の働きをしていましたからこの B が $1/A$ の働きをするものです。すると、

$$A\boldsymbol{x} = \boldsymbol{b} \Rightarrow \boldsymbol{x} = I\boldsymbol{x} = BA\boldsymbol{x} = B\boldsymbol{b}.$$

逆に、

$$\boldsymbol{x} = B\boldsymbol{b} \Rightarrow A\boldsymbol{x} = AB\boldsymbol{b} = I\boldsymbol{b} = \boldsymbol{b}.$$

これは何を言っているのでしょうか。最初の方は、$A\boldsymbol{x} = \boldsymbol{b}$ において、$\boldsymbol{x}$ は $\boldsymbol{b}$ に左から B をかければ求めることができます、ということです。後の方は、$B\boldsymbol{b}$ を $A\boldsymbol{x}$ の $\boldsymbol{x}$ に代入すると、$\boldsymbol{b}$ が得られ、$\boldsymbol{x} = B\boldsymbol{b}$ が $A\boldsymbol{x} = \boldsymbol{b}$ を満たす、行列方程式 $A\boldsymbol{x} = \boldsymbol{b}$ の解であることを言っているわけです。したがって、このような B が存在する場合は、一番最初の問題 1, 2 についても言及していることに注意して下さい。上のような B を A の逆行列といい、$B = A^{-1}$ と書きます。逆行列が次のトピックですが、逆行列について理解すると、1, 2 の解答も同時に得られることになります。それについては、またあとでまとめることにしましょう。

4.3 逆行列

連立一次方程式は、行列を用いて、$A\boldsymbol{x} = \boldsymbol{b}$ と書けるのでした。ここで、

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \ \boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \ \boldsymbol{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

さて、この方程式を一次方程式 $ax = b$ を解くのに、a で割るように、A で割ると言うことを考えられないかを考えます。そのため、以下のような定義をします。

定義 4.4 正方行列 A について、$AB = BA = I$ を満たす正方行列 B が存在するとき、A は、**可逆**である（又は、可逆行列 (invertible matrix) [**正則行列** (nonsingular matrix)] である）と言う。B を A の逆行列と言い $B = A^{-1}$ と書く。

実際 A が可逆で、$B = A^{-1}$ とすると、$A\boldsymbol{x} = \boldsymbol{b}$ の両辺に左から B をかけると、

$$B\boldsymbol{b} = BA\boldsymbol{x} = I\boldsymbol{x} = \boldsymbol{x}.$$

逆に、$\boldsymbol{x} = B\boldsymbol{b}$ とすると、$A\boldsymbol{x} = A(B\boldsymbol{b}) = (AB)\boldsymbol{b} = I\boldsymbol{b} = \boldsymbol{b}$。従って、$B\boldsymbol{b}$ が解で、解は、$B\boldsymbol{b}$ の形に限る。すなわち、$A\boldsymbol{x} = \boldsymbol{b}$ の解は、ただ一つです。すなわち、このような B が存在するのは特殊な場合であることをまず言っておきます。上の定義自体、正方行列について逆行列を定義していることに注意して下さい。

次の定理は、複雑な形をしていますが、逆行列存在の判定条件と、実際に逆行列をもとめる方法の両方を与えるものです。

定理 4.2 A を n 次正方行列、$I = I_n$ を n 次単位行列とし、$C = [A, I]$ なる、$n \times 2n$ の行列を考える。この行列 C に、行に関する基本変形を施し、既約ガウス行列に変形する。その結果を D とする。もし、$D = [I, B]$ の形になれば、$B = A^{-1}$ である。もし、D の左半分が、I で無ければ、A は、逆行列を持たない。とくに、A が逆行列を持つことと、$\mathrm{rank}\, A = n$ であることとは、同値である。

上の定理の証明はあとに回し、実際にこの方法で逆行列を求めてみましょう。

例 4.2

$$A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{bmatrix} \text{ に対して、} C = \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix}$$

とおき、次のように行の基本変形を施します。

$$\begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} \overset{[2,1;-2]}{\longrightarrow} \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & -3 & -4 & -2 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\overset{[3,1;-3]}{\longrightarrow} \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & -3 & -4 & -2 & 1 & 0 \\ 0 & -4 & -5 & -3 & 0 & 1 \end{bmatrix} \overset{[2,3;-1]}{\longrightarrow} \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & -1 \\ 0 & -4 & -5 & -3 & 0 & 1 \end{bmatrix}$$

$$\overset{[1,2;-2]}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & -1 & -2 & 2 \\ 0 & 1 & 1 & 1 & 1 & -1 \\ 0 & -4 & -5 & -3 & 0 & 1 \end{bmatrix} \overset{[3,2;4]}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & -1 & -2 & 2 \\ 0 & 1 & 1 & 1 & 1 & -1 \\ 0 & 0 & -1 & 1 & 4 & -3 \end{bmatrix}$$

$$\overset{[3;-1]}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & -1 & -2 & 2 \\ 0 & 1 & 1 & 1 & 1 & -1 \\ 0 & 0 & 1 & -1 & -4 & 3 \end{bmatrix} \overset{[2,3;-1]}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & -1 & -2 & 2 \\ 0 & 1 & 0 & 2 & 5 & -4 \\ 0 & 0 & 1 & -1 & -4 & 3 \end{bmatrix}$$

これより、A は、可逆行列で、その逆行列は、

$$A^{-1} = \begin{bmatrix} -1 & -2 & 2 \\ 2 & 5 & -4 \\ -1 & -4 & 3 \end{bmatrix}$$

となります。これが、$A^{-1}A = I = AA^{-1}$ となることを確かめてみて下さい。

上の例では、定理に書いてある方法で A^{-1} を求めましたが、こんな風に求まってしまうのは、驚きではないですか。私は最初正直感動しました。A^{-1} の成分を未知数として方程式を立て解こうとするととても大変ですから。

例 4.3

$$A = \begin{bmatrix} 5 & 1 & -1 \\ -5 & -1 & 1 \\ 2 & -1 & 0 \end{bmatrix} \text{ に対して、} C = \begin{bmatrix} 5 & 1 & -1 & 1 & 0 & 0 \\ -5 & -1 & 1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

とおき、行の基本変形を施す。

$$\begin{bmatrix} 5 & 1 & -1 & 1 & 0 & 0 \\ -5 & -1 & 1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 5 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 5 & 1 & -1 & 1 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \longrightarrow$$

これは、この後、いくら変形しても、この既約ガウス行列は、$[I, B]$ の形にならないことは、明らかである。実は、rank $A = 2$ で（ここまでで分かるのは、rank $A \leq 2$）rank $A \neq 3$ なので、A は、逆行列を持たない。

上の例からも分かるように、可逆かどうかを判定するだけなら、A をそのまま、変形して、rank A を求めれば良いことが分かりました。それには、既約ガウス行列まで変形しなくても、ガウス行列（既約ガウス行列の条件の 1-3 を満たすもの）まで変形すれば十分です。

既約ガウス行列と、ガウス行列の定義を確認しておきましょう。ガウス行列のほうは、3 までを満たすものです。

定義 4.5 次のような行列を **(既約) ガウス行列**という。

1. もし、ある行が 0 以外の数を含めば、最初の 0 でない数は 1 である。（これを先頭の 1 という。）
2. もし、すべての数が 0 であるような行が含まれていれば、それらの行は下の方によせて集められている。
3. すべてが 0 ではない 2 つの行について、上の行の先頭の 1 は、下の行の先頭の 1 よりも前に存在する。
4. (先頭の 1 を含む列の他の数は、すべて 0 である。)

定理から関連して得られる命題を数学では「系」というので、上で得たことを系として書いておこう。

系 4.3 A を正方行列とするとき、A が可逆すなわち、A に逆行列が存在することと、A から行に関する基本変形によって得られる既約ガウス行列が単位行列 I となることとは同値である。

証明. まず、G は、n 次正方行列で、既約ガウス行列とするとき、$n = \text{rank } G$ であれば、0 だけからなる行が一つもなく、$G = I$ である。逆に、$G = I$ であれば rank $G = n$ である。

A に行に関する基本変形を施して I が得られたとすると、$[A, I]$ に同じ基本変形を施すと $[I, B]$ の形の行列になる。すると定理により B は A の逆行列である。また、A に行に関する基本変形を施して得られた既約ガウス行列 G が I ではないとすると、$[A, I]$ に同じ基本変形を施すと $[G, B]$ の形の行列になる。最初に述べたことから、rank $G \neq n$。したがって、G の一番下の行はすべて 0 である。 したがって、さらに変形して既約ガウス行列を得ても、左半分は I にはならない。したがって定理より、A は逆行列を持たない。 ■

4.4 基本変形と行列

既約ガウス行列を求めるのに、行列の行に関する「基本変形」を用いましたが、この基本変形について、もう少し考えてみることにします。

もう一度、例を見てみましょう。最初、$[2,1;-2]$ を施しました。この意味は、「第 2 行に第 1 行の -2 倍を加える」と言うことでした。しかしこれは、次の行列の計算でも得られることがわかります。

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & -3 & -4 & -2 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix}$$

同様に、次のステップでは、$[3,1;-3]$ すなわち「第 3 行に第 1 行の -3 倍を加える」ことですが、これは

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & -3 & -4 & -2 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & -3 & -4 & -2 & 1 & 0 \\ 0 & -4 & -5 & -3 & 0 & 1 \end{bmatrix}$$

その後は、それぞれ、$[2,3;-1]$, $[1,2;-2]$, $[3,2;4]$, $[3;-1]$, $[2,3;-1]$ を施していますが、これらはそれぞれ、次の行列を左から順にかけても同じ効果が得られることがわかります。

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

このように行に関する基本変形は左からある行列をかけることによっても実現できます。そこで、基本変形にあわせて、そのような行列に名前をつけましょう。

$P(i;c)$**:** 第 i 行を c 倍する行列。$(c \neq 0)$

$P(i,j)$**:** 第 i 行と第 j 行を交換する行列。

$P(i,j;c)$**:** 第 i 行に第 j 行の c 倍を加える行列。

これらはもちろん考えている行列のサイズによるわけですが、たとえば上の例のように、行の数が 3 のときは、次のようになります。

$$P(2,3;-1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix},\ P(1,2;-2) = \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ P(3,2;4) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix},$$

$$P(3;-1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},\ P(2,3;-1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

上で出てこなかった行の入れ換えをする行列も書いておきましょう。

$$P(1,2) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ P(1,3) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},\ P(2,3) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

実は、これらは、I に、求めたい行に関する基本変形を施すと、求める行列がえられるという仕組みになっています。たとえば、$P(2,3;-1)$ は、I の第 2 行に第 3 行の -1 倍を加えたもの、$P(3;-1)$ は、I の第 3 行に -1 をかけたもの、$P(1,2)$ は I の第 1 行と第 2 行を入れ換えたものです。

なぜでしょうか。例えば $P = P(i,j;c)$ としましょう。$P \cdot I$ は I に $[i,j;c]$ を施したものになってほしいわけです。しかし、単位行列 I の性質から $P \cdot I = P$ でしたから、P は確かに I に $[i,j;c]$ を施したものになっているわけです。

実は、$P(i,j;c)$ は、(i,j) 成分が c であとは、I と同じ行列になっています。最初に $[i.j;c]$ などの名前を決める時、このようになることを最初から考えて決めていたわけです。わかってしまえば行列を書くのも簡単ですね。

このことを用いると、さらに以下の事が分かります。

命題 4.4 (1) $P(i;c)P(i;1/c) = P(i;1/c)P(i;c) = I$。すなわち、$P(i;c)^{-1} = P(i;1/c)$。

(2) $P(i,j)P(i,j) = I$。すなわち、$P(i,j)^{-1} = P(i,j)$。

(3) $P(i,j;c)P(i,j;-c) = I$。すなわち、$P(i,j;c)^{-1} = P(i,j;-c)$。
特に、基本変形に対応する行列、$P(i;c), P(i,j), P(i,j;c)$ はすべて可逆である。

証明. $P(i;c)P(i;1/c) = P(i;c)P(i;1/c) \cdot I$ はまず I の第 i 行を $1/c$ 倍し、次に同じ第 i 行を c 倍しますから、結局何もしないのと同じで、結果は I となります。他のものも同じですから、自分で証明してみて下さい。 ■

例 4.4 上の例で出てきた $P(2,1;-2)$ の逆行列が $P(2,1;2)$ であることを確かめてみましょう。

$$P(2,1;-2) = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ P(2,1;-2) = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

ですから、

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

これを用いて逆行列を求める計算の基本変形を行列の積で書いてみましょう。

例 4.5

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 2 & 2 \\ 3 & 2 & 1 \end{bmatrix} \text{ に対して、} C = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix}$$

とおき、行の基本変形を施す。

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} \overset{[1,2]}{=} \begin{bmatrix} 1 & 2 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} \overset{[3,1;-3]}{=} \begin{bmatrix} 1 & 2 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -4 & -5 & 0 & -3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -4 & -5 & 0 & -3 & 1 \end{bmatrix} \overset{[1,2;-2]}{=} \begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -4 & -5 & 0 & -3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -4 & -5 & 0 & -3 & 1 \end{bmatrix} \overset{[3,2;4]}{=} \begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 4 & -3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 4 & -3 & 1 \end{bmatrix} \overset{[3,-1]}{=} \begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -4 & 3 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -4 & 3 & -1 \end{bmatrix} \overset{[2,3;-1]}{=} \begin{bmatrix} 1 & 0 & 0 & -2 & 1 & 0 \\ 0 & 1 & 0 & 5 & -3 & 1 \\ 0 & 0 & 1 & -4 & 3 & -1 \end{bmatrix}$$

これより、A は、可逆行列で、その逆行列は、

$$A^{-1} = \begin{bmatrix} -2 & 1 & 0 \\ 5 & -3 & 1 \\ -4 & 3 & -1 \end{bmatrix}$$

となります。

4.5 連立一次方程式と可逆性

さて、行に関する基本変形を行列で表しましたが、これを用いていくつかのことを考えてみよう。

まずは、次の補題から。(定理の準備をする命題を補題といいます。)

補題 4.5 P, Q を 可逆な n 次正方行列とすると、P^{-1} も可逆で $(P^{-1})^{-1} = P$。また、積 PQ も可逆で $(PQ)^{-1} = Q^{-1}P^{-1}$ である。さらに、$P_1, P_2, \ldots, P_{n-1}, P_n$ をすべて可逆な n 次正方行列とすると、積 $P_nP_{n-1}\cdots P_2P_1$ も可逆で、

$$(P_nP_{n-1}\cdots P_2P_1)^{-1} = P_1^{-1}P_2^{-1}\ldots P_{n-1}^{-1}P_n^{-1}.$$

証明. $Q^{-1}P^{-1}PQ = Q^{-1}Q = I,\ PQQ^{-1}P^{-1} = PP^{-1} = I$ より、$(PQ)^{-1} = Q^{-1}P^{-1}$。一般の場合も同様。 ■

補題 4.6 A を $m \times n$ 行列とし、A に行に関する基本変形を行って、行列 B が得られたとする。すると、m 次可逆行列 P で、$PA = B$ となるものがある。

証明. 上で見たように、ある行列に行に関する基本変形を施すことは、それに対応する基本行列を左からかけることであった。A に施した基本変形に対応する基本行列を、$P_1, P_2, \ldots, P_{n-1}, P_n$ とする。$P = P_n P_{n-1} \cdots P_2 P_1$ とすると、

$$B = P_n P_{n-1} \cdots P_2 P_1 A = PA.$$

さらに $P_1, P_2, \ldots, P_{n-1}, P_n$ は、命題 4.4 で見たように可逆だから、補題 4.5 により、P は、可逆である。 ■

ここで、定理 4.2 の証明する。まず、定理を再掲する。

> A を n 次正方行列、$I = I_n$ を n 次単位行列とし、$C = [A, I]$ なる、$n \times 2n$ の行列を考える。この行列 C に、行に関する基本変形を施し、既約ガウス行列に変形する。その結果を D とする。もし、$D = [I, B]$ の形になれば、$B = A^{-1}$ である。もし、D の左半分が、I でなければ、A は、逆行列を持たない。とくに、A が逆行列を持つことと、$\mathrm{rank}\, A = n$ であることとは、同値である。

定理の証明: X, Y を n 次正方行列とし、行列 $[X, Y]$ に行に関する基本変形を施し、その基本変形に対応する基本行列を P とする。すると、行に関する基本変形を、X、Y それぞれを変形することと同じだから、結果は、$P[X, Y] = [PX, PY]$ である。このことを用いると、行列、$C = [A, I]$ に行に関する基本変形を施し、$D = [I, B]$ を得たとする。C に施した基本変形に対応する基本行列を、$P_1, P_2, \ldots, P_{n-1}, P_n$ とする。$P = P_n P_{n-1} \cdots P_2 P_1$ とすると、

$$[I, B] = D = P_n P_{n-1} \cdots P_2 P_1 C = P[A, I] = [PA, P].$$

従って、$PA = I$、$B = P$。P は、可逆行列の積だったから P も可逆。$PA = I$ より、

$$P^{-1} = P^{-1} I = P^{-1} PA = A$$

より、$B = P = A^{-1}$ である。

さて、既約ガウス行列 D の左半分を $L = PA$ とし、L が I でなければ、既約ガウス行列の定義から、L の第 m 行（一番下の行）はすべて 0 である。即ち、$\mathrm{rank}\, L = r < n$。さて、定理 3.2 は次のようなものであった。

> n 個の変数を持つ連立一次同次方程式の拡大係数行列の階数を r とする。すると、これは係数行列の階数とも等しい。$n = r$ ならば、この連立一次同次方程式の解は、$x_1 = x_2 = \cdots = x_n = 0$ のみであり、$n > r$ ならば、$n - r$ 個のパラメターを用いて解を書くことができる。とくに解は、無限個ある。

これにより、n 次列ベクトル $\boldsymbol{y} \neq \mathbf{0}$ で $L\boldsymbol{y} = \mathbf{0}$ となるものが存在する。ここで、もし A が可逆であるとすると、$L = PA$ も可逆だから、

$$\mathbf{0} = L^{-1}\mathbf{0} = L^{-1}L\boldsymbol{y} = I\boldsymbol{y} = \boldsymbol{y} \neq \mathbf{0}$$

となり、これは矛盾。従って、A は、可逆ではない。 ■

系 4.7 A, B を n 次正方行列とする。このとき、$AB = I$ ならば、A も B も可逆行列で、$BA = I$ である。可逆行列は、基本行列の積で書ける。

証明. B が可逆でないとすると、n 次列ベクトル $\boldsymbol{y} \neq \mathbf{0}$ で、$B\boldsymbol{y} = \mathbf{0}$ となるものが存在する。すると、

$$\mathbf{0} = A\mathbf{0} = AB\boldsymbol{y} = I\boldsymbol{y} = \boldsymbol{y} \neq \mathbf{0}$$

となり、矛盾。従って、B は、可逆である。これより、

$$B^{-1} = IB^{-1} = ABB^{-1} = A$$

となり、$BA = BB^{-1} = I$。最後の部分は、A の行による基本変形で、階数が、n より小さい既約ガウス行列が得られると、n 次列ベクトル $\boldsymbol{y} \neq \mathbf{0}$ で、$A\boldsymbol{y} = \mathbf{0}$ となるものが存在するから、上と同様にして、矛盾が得られる。これから、結果が得られる。 ■

連立一次方程式に戻る。

$$A\boldsymbol{x} = \boldsymbol{b}$$

と行列で表示する。拡大係数行列を、$[A, \boldsymbol{b}]$ とし、これに基本変形を次々に施すと、それに対応する基本行列の積を P として、$P[A, \boldsymbol{b}] = [PA, P\boldsymbol{b}]$ となる。これは、$PA\boldsymbol{x} = P\boldsymbol{b}$ に関する拡大係数行列である。P は、可逆であることから、次のことが分かる。

$$A\boldsymbol{x} = \boldsymbol{b} \Leftrightarrow PA\boldsymbol{x} = P\boldsymbol{b}.$$

すなわち、$\boldsymbol{x}$ が、$A\boldsymbol{x} = \boldsymbol{b}$ を満たせば、$PA\boldsymbol{x} = P\boldsymbol{b}$ を満たし、逆に、$\boldsymbol{x}$ が、$PA\boldsymbol{x} = P\boldsymbol{b}$ を満たせば、$A\boldsymbol{x} = \boldsymbol{b}$ を満たす。従って、基本変形を行っても解は、変わらないのであった。

定理 4.8 A を n 次正方行列とする。次は同値である。

(i) $BA = AB = I$ を満たす n 次正方行列 B が存在する。

(ii) $A\boldsymbol{x} = \boldsymbol{b}$ は、$\boldsymbol{b}$ を一つ決めるといつもただ一つの解を持つ。

(iii) $A\boldsymbol{x} = \mathbf{0}$ はただ一つの解を持つ。

(iv) A に行の基本変形を施し得られる既約ガウス行列はいつでも単位行列 I である。

(v) A に行の基本変形を施すと単位行列 I が得られる。

(vi) A は、基本行列のいくつかの積で書くことが出来る。

(vii) ($\det A \neq 0$。)

4.5.1 2×2 行列

$(2, 2)$ 行列についてまとめておく。

例 4.6 2×2 行列の逆行列は簡単に求められます。

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

実際、

$$AA^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix} = I$$

同様にして、

$$A^{-1}A = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = I$$

例えば、

$$\begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$$

従って、$ad-bc \neq 0$ ならば、逆行列を持つことがわかりました。逆行列を持てば、いつでも、$ad-bc \neq 0$ でしょうか。一つの方法は、行列式と言われるものを使う方法です。一般に、2×2 行列

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

について、$\det A = a_{11}a_{22} - a_{12}a_{21}$ と定義します。成分が a,b,c,d の時は、$ad-bc$ となります。すると、

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

とするとき、

$$\begin{aligned} \det(AB) &= \det\begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix} \\ &= (a_{11}b_{11}+a_{12}b_{21})(a_{21}b_{12}+a_{22}b_{22}) - (a_{11}b_{12}+a_{12}b_{22})(a_{21}b_{12}+a_{22}b_{22}) \\ &= (a_{11}a_{22}-a_{12}a_{21})(b_{11}b_{22}-b_{12}b_{21}) \\ &= \det A \det B \end{aligned}$$

であることに注意すると、$AB = I$ ならば、$\det I = 1$ ですから、

$$\det A \det B = \det I = 1$$

となります。従って、$\det A = a_{11}a_{22} - a_{12}a_{21} \neq 0$ となります。以下に命題の形でまとめておきます。

命題 4.9 2×2 行列 $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ に対して、$\det A = a_{11}a_{22} - a_{12}a_{21}$ と定義する。

(1) A, B を 2×2 行列とすると、$\det AB = \det A \det B$。

(2) A が可逆であることと、$\det A = a_{11}a_{22} - a_{12}a_{21} \neq 0$ とは、同値であり、そのとき、

$$A^{-1} = \frac{1}{\det A}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$$

それでは、行列が、2×2 よりも大きいときは、どうでしょうか。その場合も行列式と言われる det に対応するものが定義できて、大体、上の命題に対応する事が成り立ちます。それは、線形代数学 I などで勉強して下さい。

4.6 連立一次方程式まとめ

以下に連立一次方程式についてまとめる。

1. 連立一次方程式は行列方程式で表すことができる。

$$\left\{\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &=& b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &=& b_2 \\ \cdots\cdots\cdots & & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &=& b_m \end{array}\right.$$

   に対しては、

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},\ \boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},\ \boldsymbol{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

   とすると、$A\boldsymbol{x} = \boldsymbol{b}$ と書ける。

2. $A\boldsymbol{x} = \boldsymbol{b}$ の拡大係数行列は $B = [A, \boldsymbol{b}]$ であった。これに、基本変形を何回か施して、$C = [A', \boldsymbol{b}']$ となったとしよう。それは可逆行列 P をかけることと同じであった。したがって、

$$[PA, P\boldsymbol{b}] = P[A, \boldsymbol{b}] = PB = C = [A', \boldsymbol{b}'],$$

   これより、$A' = PA$, $\boldsymbol{b}' = P\boldsymbol{b}$ である。

   さて、次を証明する。

$$A\boldsymbol{x} = \boldsymbol{b} \Leftrightarrow A'\boldsymbol{x} = \boldsymbol{b}'.$$

   まず、$A\boldsymbol{x} = \boldsymbol{b}$ とする。これに、P を左からかけると、$A'\boldsymbol{x} = PA\boldsymbol{x} = P\boldsymbol{b} = \boldsymbol{b}'$ すなわち、$A'\boldsymbol{x} = \boldsymbol{b}'$ が得られた。逆に、$A'\boldsymbol{x} = \boldsymbol{b}'$ とする。P は可逆行列だったから逆行列が存在する。それを P^{-1} とかき、これを $A'\boldsymbol{x} = \boldsymbol{b}'$ に左からかけると、$P^{-1}A'\boldsymbol{x} = P^{-1}PA\boldsymbol{x} = IA\boldsymbol{x} = A\boldsymbol{x}$ 一方、$P^{-1}\boldsymbol{b}' = P^{-1}P\boldsymbol{b} = I\boldsymbol{b} = \boldsymbol{b}$ だから、$A\boldsymbol{x} = \boldsymbol{b}$ が得られた。

   これは何を言っているのだろうか。$A\boldsymbol{x} = \boldsymbol{b}$ を満たす $\boldsymbol{x}$ は $A'\boldsymbol{x} = \boldsymbol{b}'$ を満たし、逆に $A'\boldsymbol{x} = \boldsymbol{b}'$ を満たす $\boldsymbol{x}$ は $A\boldsymbol{x} = \boldsymbol{b}$ を満たす。これは、とりも直さず、宿題になっていた問題の答となっている。

   (a) C を拡大係数行列として求めた解は、本当に最初の B を拡大係数行列とする連立一次方程式の解になっている。(C の解 $\Rightarrow$ B の解)

   (b) B を拡大係数行列とする連立一次方程式の解はすべて最後の C を拡大係数行列として求めた解に含まれている。(B の解 $\Rightarrow$ C の解)

3. $\boldsymbol{x}_0$ は、$A\boldsymbol{x}_0 = \boldsymbol{b}$ を満たす n 次列ベクトルとする。$\boldsymbol{x}$ が、$A\boldsymbol{x} = \boldsymbol{b}$ を満たすとすると、

$$A(\boldsymbol{x} - \boldsymbol{x}_0) = A\boldsymbol{x} - A\boldsymbol{x}_0 = \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{0}$$

だから、$\boldsymbol{y} = \boldsymbol{x} - \boldsymbol{x}_0$ とおくと、$\boldsymbol{x} = \boldsymbol{x}_0 + \boldsymbol{y}$ で、$\boldsymbol{y}$ は、$A\boldsymbol{y} = \boldsymbol{0}$ を満たす n 次列ベクトルになっています。$A\boldsymbol{y} = \boldsymbol{0}$ の形のものすなわち、$\boldsymbol{b}$ に対応する部分が $\boldsymbol{0}$ になっているものを同次方程式とよびます。逆に、$A\boldsymbol{y} = \boldsymbol{0}$ を満たす $\boldsymbol{y}$ を取ると、$\boldsymbol{x} = \boldsymbol{x}_0 + \boldsymbol{y}$ は、$A\boldsymbol{x} = \boldsymbol{b}$ を満たす。

$$A\boldsymbol{x} = A(\boldsymbol{x}_0 + \boldsymbol{y}) = A\boldsymbol{x}_0 + A\boldsymbol{y} = \boldsymbol{b} + \boldsymbol{0} = \boldsymbol{b}.$$

この様に、$A\boldsymbol{x} = \boldsymbol{b}$ を満たす解一つと、$A\boldsymbol{x} = \boldsymbol{0}$ を満たす解すべてが分かれば $A\boldsymbol{x} = \boldsymbol{b}$ の解はすべて分かる。$\boldsymbol{x}_0$ を**特殊解** と言い、$\boldsymbol{x} = \boldsymbol{x}_0 + \boldsymbol{y}$ の形のすべての解を表すものを**一般解**と言います。

例えば一番最初に考えた連立一次方程式、

$$A\boldsymbol{x} = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 1 & 1 \\ 11 & 1 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ 17 \end{bmatrix}$$

の場合、一般解は、

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = t \cdot \begin{bmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 1 \end{bmatrix} + \begin{bmatrix} \frac{3}{2} \\ -\frac{1}{2} \\ 0 \end{bmatrix}$$

と書くことができますが、特殊解は、いろいろとあり、例えば、$\begin{bmatrix} \frac{3}{2} \\ -\frac{1}{2} \\ 0 \end{bmatrix}$ です。一方、$t \cdot \begin{bmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 1 \end{bmatrix}$ は、$A\boldsymbol{x} = \boldsymbol{0}$ を満たす解の一般形という形になっています。

4. 一般解を求めたり、解の存在非存在を決定するのには、拡大係数行列を考えて、これに行に関する基本変形を施し、ガウス行列、又は、既約ガウス行列にすることによって求めることができます。

   (a) 行に関する基本変形は 3 種類 $P(i;c)$、$P(i,j)$、$P(i,j;c)$ の基本行列という可逆な行列を左からかけることによって実現しました。これより、基本変形によって、解は変わらないことが示せました。すなわち、基本変形前の拡大係数行列に対応する解と、基本変形後の拡大係数行列に対応する解は、同じものである。

   (b) 係数行列の階数と、拡大係数行列の階数が等しいときは、解が存在し、それらが等しくないときは解は存在しない。

   (c) 解が存在する場合は、変数の数と、拡大係数行列の階数の差が、解を表すときの自由変数（パラメター）の数である。

4.7 オーディオ CD のなかの線形代数

4.7.1 誤り訂正符号

これが、今日のタイトルのオーディオ CD です。[1]CD は皆さんもご存知のように、コンパクト・ディスクの略です。最近良く利用されているのは、他にも DAT や、MD が一般的

[1]2003 年度 ICU オープンキャンパスでの模擬授業の一部を改編。

でしょうか。もっと大容量の記憶装置を持っているものも出てきています。DAT は、デジタル・オーディオ・テープ、MD は ミニ・ディスクでしょうか。これらに共通のものは、保存されているデータがすべて「デジタル」だということです。デジタルという言葉は、世の中に溢れていますね。ちょっと広辞苑で調べてみましたら、「ある量またはデータを、有限桁の数字列（例えば 2 進数）として表現すること。アナログの対語とあります。アナログは「ある量またはデータを、連続的に変化しうる物理量（電圧・電流など）で表現すること。」となっていました。デジタル化されているとは、数字になっていると言うことだと思いますが、たとえばオーディオの場合、なぜデジタルなのでしょうか。昔のレコード盤でも良いのではないでしょうか。今も、もちろんその愛好家もいるわけですが。みなさんはなぜだと思いますか。なぜ、デジタルなのでしょうか。

さて、理由は、いろいろとありますが、今日はその中の誤り訂正という話しをしようと思います。実は、デジタル化によって誤り訂正という技術が非常に有効に使われるようになっているのです。

誤り訂正？:

途中が問題ですが、エラーは、CD の場合には、ホコリや傷に対応します。ノイズが関係する場合もあります。このことからも容易に想像できるように、携帯電話や、衛星放送などの通信技術にこの技術が利用されています。皆さんは、携帯電話を英語で何と呼ぶか知っていますか。“cellular phone” とか “cell phone” と呼びますね。“portable telephone” とか、“mobile phone” ということばも一部の地域では使われているようですが。これは地域を小さなセル（小さく区切った部屋）に分けて、その中にアンテナをおいて通信をするわけです。この話しも誤り訂正の基本理論ととても関係があるので、時間があればあとで少しお話します。

4.7.2 Hamming Code:

ともかく、どんなふうになるかちょっとやってみましょう。

最初に必要なのは、二つの行列です。

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

さて、データは 2 進 4 桁とします。0, 1 が 4 つ並んだものです。今日は、$(3, 8)$ という二つの数を取り上げてみましょう。ここでは、もともと数を扱いましたが、これが音のデータだったりするのです。この 2 進表示は、$(0011), (1000)$ となります。一番下の位は、

$1 = 2^0$、次は $2 = 2^1$、次は、$4 = 2^2$、一番上の位が $8 = 2^3$ を表します。こういうことは知っているよと言う人はどのくらいいますか。これは 2 進表示といいますが、それでは、負の数や、少数は 2 進では、どうあらわしたらよいかわかりますか。考えてみて下さい。今日は、それは必要ありませんから、先にいきましょう。

これを CD に書き込むと、noise 汚れや傷がついて、0 が 1 または、1 が 0 に変わると、他の数を表すことになりますから、これにちょっと付け加えて送ります。a のかわりに、$a \cdot G$ を使います。0 と 1 の世界の足し算を、次のように約束しておきます。

$K = \{0, 1\}$ の足し算：

$$0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1,\ 1 + 1 = 0$$

そして、$(0011) \cdot G$ は、G の第 3 行目と第 4 行目を、それぞれの列ごとに、足すと考えて下さい。桁あがりなどはありませんよ。$1 + 1 = 0$ ですから。すると、

$$\begin{aligned} 3 &: \ (0011) \cdot G = (0010110) + (0001111) = (0011001) \\ 8 &: \ (1000) \cdot G = (1000011) \end{aligned}$$

0, 1 のかけ算を

$$0 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 1 \cdot 0 = 0,\ 1 \cdot 1 = 1$$

としておけば、これは、行列のかけ算をしていることだということもわかると思います。

さて、noise があり、これらが変わったとして、そこで得たものが x だとしましょう。このとき、今度は、$x \cdot H$ を計算します。これも同じです。1 のあるところの行を足すと考えて下さい。例えば、

$$(0011001) \to (0011011) \cdot H = (011) + (100) + (110) + (111) = (110)$$

これは 2 進数の 6 を表しますから 6 番目にノイズが入ったことがわかります。

ではなぜうまくいくのかを考えてみましょう。

(4–1)

	u	$u \cdot G$	wt
0	0000	0000000	0
1	0001	0001111	4
2	0010	0010110	3
3	0011	0011001	3
4	0100	0100101	3
5	0101	0101010	3
6	0110	0110011	4
7	0111	0111100	4
8	1000	1000011	3
9	1001	1001100	3
A	1010	1010101	4
B	1011	1011010	4
C	1100	1100110	4
D	1101	1101001	4
E	1110	1110000	3
F	1111	1111111	7

$$
\begin{aligned}
C &= \{u \cdot G \mid u \in K^4\} \\
&= \left\{ \begin{array}{llll}
(0000000), & (0001111), & (0010110), & (0011001), \\
(0100101), & (0101010), & (0110011), & (0111100), \\
(1000011), & (1001100), & (1010101), & (1011010), \\
(1100110), & (1101001), & (1110000), & (1111111)
\end{array} \right\} \subset V = K^7
\end{aligned}
$$

とすると、

$$c + c' \in C \ \text{ for every } c, c' \in C$$

となっています。保存されるのは、C の要素ということになります。Code word と呼ばれますから、その全体を C で表しています。このことを、C は足し算に関して閉じているといいます。

実は、$\cdot$ という演算が、

(4–2)
$$u \cdot G + v \cdot G = (u + v) \cdot G$$

を満たすことがわかると、その理由もわかります。

さらに、$c \in C$ とすると、いつでも、

$$c \cdot H = O$$

であることがわかります。実は、G の各行 g について、$g \cdot H = (000)$ であることを確かめれば、あとは、性質 (4–2) からわかります。行列の積を使えば、

$$G \cdot H = O$$

を確かめて、あとは、$c \cdot H = (u \cdot G)H = d \cdot (GH)$ ということからもわかります。結局、普通に送られたものに、H をかけてみると (000) がえられるということです。これが送られてくれば、0 列目にあやまりがありますよ。という意味だったわけです。さて、ここで、

$$
\begin{aligned}
e_1 &= (1000000) \\
e_2 &= (0100000) \\
e_3 &= (0010000) \\
e_4 &= (0001000) \\
e_5 &= (0000100) \\
e_6 &= (0000010) \\
e_7 &= (0000001)
\end{aligned}
$$

としましょう。$c \in C$ とし、i 番目の bit に error が起こった時は、$c + e_i$ が得られるので、$(c + e_i) \cdot H$ を計算すると、性質 (4–2) から、$e_i \cdot H$ が得られ、H の 第 i 列めが得られます。しかし、 H の第 i 列は、2 進数の i を表しているから、i を特定することができる。したがって、一箇所にしか error が起こっていない時は、その位置を特定し、修正することが可能だということです。

なぜ、うまくいくかを、他の面から考えてみましょう。$x, y \in V = K^7$ とし、

$$\mathrm{dist}(x, y) = \text{ことなる成分の個数}$$

で定義すると、

$$\mathrm{dist}(x,y) = \mathrm{dist}(x-y,0) = x-y \text{ のゼロでない成分の個数} = wt(x-y)$$

となります。$c, c' \in C$ を $c \neq c'$ とすると、$c - c'$ はゼロではない、C の要素だから、表から $\mathrm{dist}(x-y,0) \geq 3$ となっている。つまり C の要素はお互いに、距離 3 以上離れているので、一箇所ぐらい変わっても、もとの位置を特定できる。という関係になっているのです。

冗長さが、誤り訂正の働きをしてくれる。実は、これは、日常生活の中でもあることで、自然言語を使う場合、冗長さを持つことにより、完全に聞きとることができなくても、また話者のことばが完全ではなくても、必要な内容は伝えることができる場合が多い。

余談ですが、DNA に含まれる塩基列の解明が進み、そのなかに組み込まれている遺伝情報が読みとれるようになってきていますが、そのなかで遺伝情報に関係していない、intron という部分がかなりの部分を占めています。しっかりとは理解できていませんが、細胞内で合成するタンパク質についての情報をもった RNA を転写して DNA からつくり出す時に使われない部分がたくさんあるということではないかと思います。高等生物であっても、下等生物であっても、遺伝子の数はそれほどちがわないが、intron は大分違っている。これは、進化の過程の「試行錯誤」のなかで不要になったもの、ともいわれているようですが、ひょっとして、今ここでお話した、誤り訂正などのために働いてはいないかなと夢のような話しも生物のかたと話す時に考えています。

CD の符号:

今、紹介したのは Hamming (7,4,3) 符号というものです。1950 年ごろに作られたものです。長さが 7、情報の場所が 4 桁、最小距離が 3 と言う意味です。どういう符号がいい符号でしょうか。長さに対して、情報の場所が大きくかつ最小距離も大きいものがよい符号です。

実際に CD や MD で使われているのは、2 重符号化 Reed-Solomon Code と言われているものです。最初に、$K = \{0,1\}$ に足し算とかけ算を定義しましたが、Read-Solomon Code の場合には、要素が 2^m の集合に、四則演算を定義します。四則演算が定義された集合を体といいますが、これをつかって符号を定義するのです。それには、もう少し、複雑な代数が必要です。

4.7.3 Perfect Code:

$C \subset K^n$ 長さが n の e-重誤り訂正符号。C の要素のお互いの距離が $d = 2e+1$ 以上離れていることが必要です。$c = (c_1, c_2, \ldots, c_n) \in C$ とすると、x との距離が 1 ということは、x と成分がどこか一つことなるということでしたから、そのようなものの数は、n 個。距離が 2 離れている点は、${}_nC_2$ だけありますから、そのようにして考えると、

$$\bigcup_{c \in C} B_e(c) \subset V \quad \text{(disjoint)}$$

から

$$|C| \cdot \sum_{i=0}^{e} {}_nC_i \leq |K^n| = 2^n$$

となっているはずです。今の場合は、$e = 1$、$d = 3$ だから

$$2^4 \cdot \sum_{i=0}^{1} {}_7C_i = 2^4(1+7) = 2^7 = |K^7|$$

ですから、単に不等式になっているのではなく、等式になっているわけです。これは、各 C の要素から距離が $0, 1, \ldots, e$ の点を合わせるとすべての K^n の点が得られるという場合です。この様に上の等式を満たす符号 (code) を完全符号 (perfect code) と呼びます。上の Hamming (7,4,3) 符号は perfect code の例になっています。

長さ n、符号の次元が k、最小距離が d である（2 元）線形符号を (n, k, d) 符号といいます。$d \geq 2e+1$ のとき、この符号は e 重の誤り訂正をすることができます。

Golay Code:

もう一つすごい符号を紹介しましょう。

$$G = \left[\begin{array}{cccccccccccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&1&1&1&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&1&1&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&1&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&0&1&1\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&1&0&1&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1
\end{array}\right]$$

11 で割ったあまりを考え、あるかずの 2 乗になっているものを考えると

$$\{0\} \cup \{1, 3, 4, 5, 9\}$$

これを使って作った行列です。この G を使って作った Binary Golay Code (23, 12, 7) は 3 重誤り訂正符号。

$$2^{12}(1 + {}_{23}C_1 + {}_{23}C_2 + {}_{23}C_3) = 2^{12}(1 + 23 + 253 + 1771) = 2^{12} \cdot 2^{11} = 2^{23}$$

Perfect Codes はあまり存在しないことがわかっています。

Theorem 非自明な（Binary) e-error correcting code ($e \geq 1$) は、Binary Golay Code か、Hamming code と同じパラメター $((2^m - 1, 2^m - m - 1, 3))$ を持つものしか存在しない。

4.7.4 携帯電話と球詰め問題:

皆さんは、携帯電話は、英語で “cellular phone” とか “cell phone” と呼びますね。これは地域を小さなセル（小さく区切った部屋）に分けて、その中にアンテナをおいて通信

をするわけです。こちらには、ある円であまり重なりはないけれど、すべてをおおいたいという問題があります。先ほどの符号の問題は、重なりがない円をどれだけたくさんいれることができるかという問題を考えていたとも言えます。どちらも実は、球詰め問題という同じ問題に関係しています。大きな箱にピンポン球をたくさんいれたい。どのくらいの密度でいれることができるだろうか。という問題は、まだ解決がされていません。キッシングナンバーも、1, 2, 3, 8, 24 が解決していますが、それ以外については、わかっていません。情報科学とも関係の深いこれらの問題が、数学的にもとても深い問題と関係していると言うのは、とても面白いことだとは思いませんか。

人間の問題: 今日お話した、符号理論は、暗号理論 (cryptography) [security と関係] とともに情報科学・数学で重要な分野をなしています。わたしは、この符号理論の背景にあるものが好きです。

誤りは避けられない。誤りを指摘されるのは、いやだが、誤りをそっと直しておいてくれるのは何とも嬉しい。通常は無駄なものが癒しを与えてくれる。というのは人間的だと思いませんか。効率が重視される工学でも、世の中の実際の問題を考える時には、われわれが完全ではないということ、人間についてよくわかっていないと、すぐ問題がおこってしまうのです。